PATENT
Customer No. 25537
Attorney Docket No. 96-3-512CON1CP2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)	
)	
W. David SHAMBROOM)	Group Art Unit: 2131
)	
Application No.: 09/759,100)	Examiner: Kaveh Abrishamkar
)	
Filed: January 12, 2001)	
)	
For: PLATFORM-NEUTRAL SYSTEM)	Confirmation No.: 1842
AND METHOD FOR PROVIDING)	
SECURE REMOTE OPERATIONS)	
OVER AN INSECURE)	
COMPUTER NETWORK)	

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

APPEAL BRIEF UNDER BOARD RULE § 41.37

In support of the Notice of Appeal filed August 24, 2006, and further to Board

Rule 41.37, Appellant presents this brief and encloses herewith a check for the fee of

$500.00 required under 37 C.F.R. § 1.17(c). This Appeal Brief is being timely filed on or

before one month from the mailing date of a Panel Decision from Pre-Appeal Brief

Review.

This Appeal responds to the April 4, 2006, final rejection of claims 1-36.

If any additional fees are required or if the enclosed payment is insufficient,

Appellant requests that the required fees be charged to Deposit Account No. 06-0916.

Table of Contents

I.   Real Party In Interest

The real party in interest is Verizon Laboratories, Inc., the assignee of record.

II.   Related Appeals and Interferences

There are currently no other appeals or interferences, of which Appellant, Appellant's legal representative, or Assignee are aware, that will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status Of Claims

In the Final Office Action mailed March 9, 2006, the Examiner rejected claims 1-36 under 35 U.S.C. § 103(a) as unpatentable over *Krajewski* (U.S. Patent No. 5,590,199) in view of *Fischer* (U.S. Patent No. 5,005,200).

The final rejection of claims 1-36 are being appealed and a list of the claims on appeal is found in the attached Claims Appendix.

Furthermore, each claim of this patent application is separately patentable, and upon issuance of a patent will be entitled to a separate presumption of validity under 35 U.S.C. § 282.

## IV.	Status Of Amendments

The claims were most recently amended in a Reply to Office Action filed January 10, 2006, in reply to a non-final Office Action mailed August 9, 2005. No amendments have been submitted subsequent to the Final Office Action mailed April 4, 2006.

V. Summary Of Claimed Subject Matter

a. Claim 1

Independent claim 1 is directed to a method of enhancing the security of a message sent by a principal from a client computer through a network server to a destination server. In the method, steps are performed for obtaining by the client computer credentials for authorizing the principal from a validation center (for example, Fig. 3, p. 18, line 16 - p. 20, line 3); establishing a first secure connection for exchanging data between the client and the network server (for example, Figs. 1 and 2, p. 15, line 14 - p. 17, line 22); transmitting from the client computer to the network server over the first secure connection the principal-authenticating credentials and the message (for example, Fig. 3, p. 17, line 19-22 and p. 20, lines 5-14); and transmitting the principal-authenticating credentials from the network server to the validation center (for example, Fig. 3, p. 18, lines 16-21).

Further, in the method, steps are performed for transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials (for example, Fig. 3, p. 18, line 21 - p. 19, line 10); verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server (for example, Figs. 8, 9a and 9b, p. 32, line 21 - p. 34, line 7); establishing a second secure connection for exchanging data between the network server and the destination server based on the digital certificate (for example, Figs. 8 and 9c, p. 34, line 8 - p. 35, line 6) ; and

7

transmitting the message from the network server to the destination server over the second secure connection (for example, Fig. 8, p. 35, lines 6-7).

<u>b.</u>   <u>Claim 23</u>

Independent claim 23 is directed to a method of providing a remote interactive login connection for a principal from a client computer through a network server to a destination server. In the method, steps are performed for obtaining credentials for authorizing the principal from a validation center (for example, Fig. 3, p. 18, line 16 - p. 20, line 3); establishing a first secure connection for exchanging data between the client and the network server (for example, Figs. 1 and 2, p. 15, line 14 - p. 17, line 22); transmitting from the client computer to the network server over the first secure connection the principal-authenticating credentials (for example, Fig. 3, p. 17, lines 19- 22); and transmitting the principal-authenticating credentials from the network server to the validation center (for example, Fig. 3, p. 18, lines 16 - 21).

Further, in the method, steps are performed for transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials (for example, Fig. 3, p. 18, line 21 - p. 19, line 10); verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server (for example, Figs. 8, 9a, and 9b, p. 32, line 21 - p. 34, line 7); establishing a second secure connection for exchanging data between the network server and the destination server based on the digital certificate (for example, Figs. 8 and 9c, p. 34, line 8 - p. 35, line 6); and executing a command interpreter in the destination server wherein the command interpreter may

8

execute commands sent by the client computer via the network server over the second secure connection (for example, Figs. 8 and 9d, p. 35, lines 15-20).

c. Claim 24

Independent claim 24 is directed to a computer system for enhancing the security of one or more messages sent by a principal. The computer system may comprise a client computer for transmitting principal-authenticating credentials and the one or more messages (for example, Fig. 3, p. 18, line 16 - p. 20, line 3); a gateway computer operatively connected to the client computer, the gateway computer receiving principal-authenticating credentials and the one or more messages from the client computer (for example, Figs. 1-3, p. 15, line 14 - p. 17, line 22); and a validation computer operatively connected to the gateway computer and capable of receiving the principal-authenticating credentials from the gateway computer and of transmitting permission data on the principal-authenticating credentials to the gateway computer (for example, Fig. 3, p. 18, line 16 - p. 19, line 10).

The computer system may further comprise one or more host computers operatively connected to the gateway computer and operating on any computer platform, wherein, based on the permission data, the gateway computer establishes a secure connection with at least one of the one or more host computers, and wherein the gateway computer transmits the one or more messages to at least one of the host computers over the secure connection (for example, Figs. 8 and 9a-c, p. 34 line 8 - p. 35, line 7).

<u>d.</u>   <u>Claim 29</u>

Independent claim 29 is directed to a computer system for providing a remote interactive login connection. The computer system may comprise a client computer for transmitting principal-authenticating credentials and a message (for example, Fig. 3, p. 18, line 16 - p. 20, line 3); a gateway computer operatively connected to the client computer, the gateway computer receiving the principal-authenticating credentials and the message from the client computer (for example, Figs. 1-3, p. 15, line 14 - p. 17, line 22); and a validation computer operatively connected to the gateway computer and capable of receiving the principal-authenticating credentials from the gateway computer and of transmitting permission data based on the principal-authenticating credentials to the gateway computer (for example, Fig. 3, p. 18, line 16 - p. 19, line 10).

The computer system may further comprise one or more host computers operatively connected to the gateway computer and operating on any computer platform, wherein, based on the permission data, the gateway computer establishes a secure connection with the host computer, and transmits the message to the host computer over the secure connection (for example, Figs. 8 and 9a-c, p. 34, line 8 - p. 35, line 7).

<u>e.</u>   <u>Claim 36</u>

Independent claim 36 is directed to a computer program product for use with a computer system, the computer program product comprising a computer readable storage medium and a computer program stored therein for carrying out a process comprising obtaining by the client computer credentials for authorizing the principal from

10

a validation enter (for example, Fig. 3, p. 18, line 16 - p. 20, line 3); establishing a first secure connection for exchanging data between a client and a network server (for example, Figs. 1 and 2, p. 15, line 14 - p. 17, line 22); transmitting from the client computer to the network server over the first secure connection the principal-authenticating credentials and the message (for example, Fig. 3, p. 17, line 19-22 and p. 20, lines 5-14); and transmitting the principal-authenticating credentials from the network server to the validation center (for example, Fig. 3, p. 18, lines 16-21).

The process may also comprise transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials (for example, Fig. 3, p. 18, line 21 - p. 19, line 10); verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server (for example, Figs. 8, 9a and 9b, p. 32, line 21 - p. 34, line 7); establishing a second secure connection for exchanging data between the network server and a destination server based on the digital certificate (for example, Figs. 8 and 9c, p. 34, line 8 - p. 35, line 6); and transmitting the message from the network server to the destination server over the second secure connection (for example, Fig. 8, p. 35, lines 6-7).

VI. Grounds of Rejection

A.   Claims 1-36 stand rejected under 35 U.S.C. § 103(a) as unpatentable over *Krajewski* (U.S. Patent No. 5,590,199) in view of *Fischer* (U.S. Patent No. 5,005,200).

VII. Argument

The rejections of claims 1-36 under 35 U.S.C. § 103(a)

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, the prior art reference or references, taken alone or combined, must teach or suggest each and every element recited in the claims. *See* M.P.E.P. § 2143.03. Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine the references in a manner resulting in the claimed invention. *See* M.P.E.P. § 2143. Third, a reasonable expectation of success must exist. *See* M.P.E.P. § 2143.02. Moreover, each of these requirements must "be found in the prior art, and not based on applicant's disclosure." M.P.E.P. § 2143. For at least the following reasons, Appellant respectfully submits the Examiner has failed to establish a *prima facie* case of obviousness in connection with the rejections of claims 40-46, 48-57, 59-68, 70-72, and 76-84.

> a. **The rejection of claims 1-36 under 35 U.S.C. § 103(a) must be reversed because *Krajewski* and *Fischer* do not teach or suggest, at least the claimed network server and destination server.**

(i)   Claim 1

Appellant respectfully traverses the rejection of claim 1 under 35 U.S.C. § 103(a) because *Krajewski* and *Fischer* do not teach or suggest each and every recitation of claim 1. This claim recites a method of enhancing the security of a message sent by a principal from a client computer through a network server to a destination server, using communication between a validation center and the network server. The client

computer transmits principal-authenticating credentials to the network server, as well as a message for transmitting to the destination server. The network server in turn transmits the principal-authenticating credentials to the validation center, which in return transmits permission data to the network server. The network server then verifies the authorization of the principal, and transmits the message to the destination server.

In contrast, *Krajewski* teaches an untrusted workstation 14 used as a client, a service 20 (referred interchangeably as a computer, network, and system server/service), and a Kerberos authorization server (KAS) 32 (*Krajewski* Fig. 3 and col. 5, lines 46-54). Service 20 executes a program referred to as "server Kerberos" that interacts with KAS 32 (*Krajewski* Fig. 4, col. 5 lines 39-45). The untrusted workstation 14 performs some authentication processing using a locally available smart card 30 (*Krajewski* col. 6, lines 38-67).

This is different from the claimed method, because messages transmitted in *Krajewski* are not transmitted by a client to a network server and in turn to a destination server. Instead, messages are directly transmitted from the client computer 14 to the service 20. There is simply no device in *Krajewski* analogous to the claimed network server, which communicates with a client computer, validation center, and a destination server to send a message from the client computer to the destination server.

The Examiner has applied the teachings of *Krajewski* incorrectly, and inconsistently, during the prosecution of this application. Consider first the non-final Office Action mailed August 9, 2005. Referring to the claim language "transmitting the principal authenticating credentials from the network server to the validation center," the Examiner cites portions of *Krajewski* disclosing transferring a ticket from the client to the

smart card 30 (non-Final Office Action p. 3 ¶ 2 line 6 - p. 4 line 2), seeming to allege

that the smart card 30 corresponds to the claimed network server. However, in the text

accompanying the citation, the Examiner appears to indicate that the service 20, and

not the smart card 30, corresponds to the claimed network server. At the end of this

very same paragraph, the Examiner appears to equate the service 20 with the claimed

destination server (non-Final Office Action page 4, lines 11-13).

In the Final Office Action mailed April 4, 2006, the Examiner again failed to

provide a coherent explanation of how the devices in *Krajewski* correspond to the

claimed network and destination server. In response to Appellant's arguments, the

Examiner appears to reassert that the service 20 corresponds to the claimed network

server, but then asserts that the server Kerberos corresponds to the claimed destination

server (Final Office Action p. 2 ¶ 4, lines 11-12). Note that claim 1 recites "exchanging

data between the network server and the destination server based on the digital

certificate," but *Krajewski* clearly shows the server Kerberos located on the service 20

(see Fig. 4). The Examiner's mapping appears to assert the unusual position that the

service 20 uses a digital certificate in order to communicate with its own software.

In an Advisory Action dated July 11, 2006, the Examiner appeared to retreat from

his position that server Kerberos constitutes the claimed destination server, instead

alleging only that *Fischer* discloses the claimed destination server. However, note that

in both the non-Final and Final Office Actions, the Examiner relied on *Fischer* to teach

the claimed digital certificate, not the destination server. If the Examiner's position is

now that *Krajewski* does not teach the claimed destination server, but rather *Fischer*

does so, Appellant has not had an opportunity to address this position.

In sum, at various times the Examiner has alleged that service 20 corresponds to both the claimed network or destination server, has alleged that the smart card 30 corresponds to the claimed network server, and has alleged that the server Kerberos corresponds to the claimed destination server. Finally, in the Advisory Action, the Examiner appears to indicate that *Fischer*, and not *Krajewski*, teaches the claimed destination server.

In any event, even assuming *Fischer* teaches the claimed destination server (a position Appellant does not concede), *Krajewski* still fails to teach or suggest the claimed network server. As discussed above, the Examiner has applied both *Krajewski*'s smart card 30 and service 20 as allegedly disclosing the claimed network server. Neither interpretation of *Krajewski* is correct.

Regarding the Examiner's position that the smart card 30 corresponds to the claimed network server, Appellant simply notes that Fig. 3 of *Krajewski* clearly illustrates that the smart card does not have a communication link to the network 18, and thus communicates only with untrusted workstation 14. Thus, the smart card 30 cannot correspond to the claimed network server, which communicates with a client computer, validation center, and a destination server.

Regarding the Examiner's position that the server 20 corresponds to the claimed network server, Appellant simply notes that server 20 does not communicate with KAS 32. Thus, even assuming KAS 32 corresponds to the claimed validation center (a position Appellant does not concede), the server 20 cannot correspond to the claimed network server which "transmit[s] the principal-authenticating credentials ... to the validation center."

16

Regarding the Examiner's position that the server Kerberos corresponds to the claimed destination server (Final Office Action p. 2 ¶ 4, lines 11-12), this position is equally untenable. As discussed above and at col. 2, lines 37-51 of *Krajewski*, "server Kerberos" is software, and not a device such as a server. In the context of *Krajewski*'s disclosure, server Kerberos is authentication software running on server 20.

This position is even more untenable when considered in the context of the Examiner's mappings of the claimed network server to devices in *Krajewski*. The claimed network server "transmit[s] the message from the network server to the destination server over the second secure connection." Thus, if, as the Examiner alleges, the smart card 30 corresponds to the claimed network server, *Krajewski* would need to disclose some communication between the smart card 20 and server Kerberos (the alleged destination server). *Krajewski* does not, clearly indicating that the smart card communicates with <u>client</u> Kerberos (*Krajewski* col. 6, lines 53-57). Conversely, were the server 20 to correspond to the claimed network server, *Krajewski* would need to teach transmitting a message from server 20 to it's own server Kerberos software, over a secure connection. Such a teaching is not found in *Krajewski*.

Fischer does not make up for the above noted deficiencies of *Krajewski*. Indeed, the Examiner relies on *Fischer* primarily for *Fischer*'s teachings regarding digital certificates (*See* Final Office Action, page 5). *Fischer* discloses a public key cryptographic system with a "hierarchy of nested certifications and signatures ... which indicate the authority and responsibility levels of the individual whose signature is being certified." (*Fischer*, abstract). *Fischer*, however, also fails to disclose a device analogous to the claimed network computer or destination computer.

Because *Krajewski* or *Fischer*, alone or in combination, fail to teach or suggest at least the claimed network server or destination server as recited in claim 1, Appellant submits the Examiner has not established a *prima facie* case of obviousness. For at least these reasons, Appellant respectfully requests that the Board reverse the rejection of claim 1 under 35 U.S.C. § 103(a) and allow the claim.

(ii)   Claims 2-22

Claims 2-22 depend from claim 1. As explained, claim 1 is distinguishable from *Krajewski* and *Fischer*. Accordingly, claims 2-22 are also distinguishable from these references for at least the same reasons set forth above in connection with claim 1. Therefore, Appellant respectfully requests that the Board reverse the rejection of these claims under 35 U.S.C. § 103(a) and allow the claims.

(iii)   Claims 23, 24, 29, and 36

The Examiner rejects claims 23, 24, 29, and 36 for reasons consistent with the rejection of claim 1. (*See Final Office Action,* pages 15-19, 22-24, and 27-29) As explained, claim 1 is distinguishable from *Krajewski* and *Fischer*. Accordingly, claims 23, 24, 29, and 36 are also distinguishable from these references for at least the same reasons set forth above in connection with claim 1. Therefore, Appellant respectfully requests that the Board reverse the rejection of claims 23, 24, 29, and 36 under 35 U.S.C. § 103(a) and allow the claims.

(iv)   Claims 25-28 and 30-35

Claims 25-28 and 30-35 depend from claims 24 and 29, respectively. As explained, claims 24 and 29 are distinguishable from *Krajewski* and *Fischer*. Accordingly, claims 25-28 and 30-35 are also distinguishable from these references for

at least the same reasons set forth above in connection with claims 24 and 29.

Therefore, Appellant respectfully requests that the Board reverse the rejection of these

claims under 35 U.S.C. § 103(a) and allow the claims.
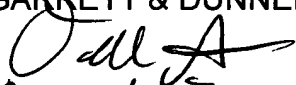
VIII.   Conclusion

For the reasons given above, pending claims 1-36 are allowable and reversal of

the Examiner's rejection is respectfully requested.

To the extent any extension of time under 37 C.F.R. § 1.136 is required to obtain

entry of this Appeal Brief, such extension is hereby respectfully requested. If there are

any fees due under 37 C.F.R. §§ 1.16 or 1.17 which are not enclosed herewith,

including any fees required for an extension of time under 37 C.F.R. § 1.136, please

charge such fees to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: October 30, 2006   By: _Reg. No. 34,731_____

for Jeffrey A. Berkowitz
Reg. No. 36,743

Appendix A: Listing of Claims Under Rule 41.37(c)(1)(viii)

1. (Previously Presented) A method of enhancing the security of a message sent by a principal from a client computer through a network server to a destination server, comprising the steps of:

    (a)   obtaining by the client computer credentials for authorizing the principal from a validation center;

    (b)   establishing a first secure connection for exchanging data between the client and the network server;

    (c)   transmitting from the client computer to the network server over the first secure connection the principal-authenticating credentials and the message;

    (d)   transmitting the principal-authenticating credentials from the network server to the validation center;

    (e)   transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials;

    (f)   verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server;

    (g)   establishing a second secure connection for exchanging data between the network server and the destination server based on the digital certificate; and

    (h)   transmitting the message from the network server to the destination server over the second secure connection.

2. (Previously Presented) The method of claim 1, wherein the establishing step (b) utilizes the Secure Sockets Layer (SSL) protocol.

3. (Previously Presented) The method of claim 1, wherein the establishing step (b) further comprises the substeps of:

transmitting from the network server to the client server a network server key associated with a public-private key pair and a known cryptographic algorithm;

transmitting from the client server to the network server a session key encrypted using the known cryptographic algorithm and the network server key; and

transmitting from the network server to the client server information encrypted using the known cryptographic algorithm and the session key to authenticate the network server to the client server.

4. (Original) The method of claim 1, wherein the establishing step (g) utilizes the Secure Sockets Layer (SSL) protocol.

5. (Original) The method of claim 1, wherein the establishing step (g) further comprises the substeps of:

transmitting from the destination sever to the network server a destination server key associated with a public-private key pair and a known cryptographic algorithm;

transmitting from the network server to the destination server a session key encrypted using the known cryptographic algorithm and the destination server key; and

transmitting from the destination server to the network server information encrypted using the known cryptographic algorithm and the session key to authenticated the destination server to the network server.

6. (Previously Presented) The method of claim 1, wherein the obtaining step (a) further comprises the substeps of:

sending a request for credentials for the principal to the validating center;

receiving the credentials for the principal for from the validation center; and

storing the credentials in the client computer.

7. (Original) The method of claim 1 wherein the principal-authenticating credentials comprise a ticket-granting ticket and a session key.

8. (Original) The method of claim 7 wherein the transmitting step (d) further comprises the substep of:

transmitting from the network server to the validating center a ticket-granting ticket and an authenticator.

9. (Original) The method of claim 8 wherein the ticket-granting ticket comprises a session key encrypted with a permanent key for the validation center.

10. (Original) The method of claim 9 wherein the authenticator is a data structure encrypted using the session key.

11. (Original) The method of claim 10 wherein the transmitting step (e) further comprises the substep of:

decrypting the ticket-granting ticket at the validation center to extract a session key.

21

12. (Original) The method of claim 11 wherein the permission data comprises an authenticator.

13. (Original) The method of claim 12 wherein the authenticator comprises a data structure encrypted with the session key.

14. (Original) The method of claim 1 further comprising the steps of:

transmitting a request for a server ticket from the network server to the validation center;

creating a server ticket for the network server at the validation center; and

receiving the server ticket from the validation center at the network server.

15. (Original) The method of claim 5 wherein the verifying step (f) further includes the substeps of:

extracting an access control list and verifying that the principal is authorized to access a digital certificate and a destination server key; and

issuing a digital certificate and a destination server key.

16. (Original) The method of claim 15 wherein the digital certificate conforms with the X.509 standard.

17. (Original) The method of claim 1 wherein the establishing step (g) further comprises the substep of:

establishing a secure connection from the network server to more than one destination server.

18. (Original) The method of claim 17 wherein each connection between the network server and a destination server is managed by a separate remote command execution client.

19. (Original) The method of claim 1 wherein the validation center utilizes a Kerberos protocol.

20. (Original) The method of claim 1 wherein the message comprises command data.

21. (Original) The method of claim 20 wherein the command data comprise a remote user name, and a destination server list, and a command.

22. (Original) The method of claim 1 further comprising the step of temporarily storing the principal-authenticating information.

23. (Previously Presented) A method of providing a remote interactive login connection for a principal from a client computer through a network server to a destination server, comprising the steps of:

22

(a)   obtaining credentials for authorizing the principal from a validation center;

(b)   establishing a first secure connection for exchanging data between the client and the network server;

(c)   transmitting from the client computer to the network server over the first secure connection the principal-authenticating credentials;

(d)   transmitting the principal-authenticating credentials from the network server to the validation center;

(e)   transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials;

(f)   verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server;

(g)   establishing a second secure connection for exchanging data between the network server and the destination server based on the digital certificate; and

(h)   executing a command interpreter in the destination server wherein the command interpreter may execute commands sent by the client computer via the network server over the second secure connection.

24. (Previously Presented) A computer system for enhancing the security of one or more messages sent by a principal comprising:

a client computer for transmitting principal-authenticating credentials and the one or more messages;

a gateway computer operatively connected to the client computer, the gateway computer receiving principal-authenticating credentials and the one or more messages from the client computer;

a validation computer operatively connected to the gateway computer and capable of receiving the principal-authenticating credentials from the gateway computer and of transmitting permission data on the principal-authenticating credentials to the gateway computer; and

one or more host computers operatively connected to the gateway computer and operating on any computer platform,

wherein, based on the permission data, the gateway computer establishes a secure connection with at least one of the one or more host computers, and

wherein the gateway computer transmits the one or more messages to at least one of the host computers over the secure connection.

25. (Original) The system of claim 24 wherein the gateway computer further comprises a gateway certificate server for transmitting the principal-authenticating credentials to the validation center and for receiving the permission data from the validation computer.

26. (Original) The system of claim 24 wherein the gateway computer further comprises one or more remote command execution clients for establishing one or more secure connections to the one or more host computers based on the permission data.

27. (Original) The system of claim 24 wherein each of the one or more host computers further comprises a host proxy and execution server for establishing a secure connection between each of the one or more host computers and the gateway computer.

28. (Original) The system of claim 27 wherein the host proxy and execution server executes a command interpreter for executing commands contained in the one or more messages.

29. (Previously Presented) A computer system for providing a remote interactive login connection comprising:

a client computer for transmitting principal-authenticating credentials and a message;

a gateway computer operatively connected to the client computer, the gateway computer receiving the principal-authenticating credentials and the message from the client computer;

a validation computer operatively connected to the gateway computer and capable of receiving the principal-authenticating credentials from the gateway computer and of transmitting permission data based on the principal-authenticating credentials to the gateway computer; and

one or more host computers operatively connected to the gateway computer and operating on any computer platform,

wherein, based on the permission data, the gateway computer establishes a secure connection with the host computer, and transmits the message to the host computer over the secure connection.

30. (Original) The system of claim 29 wherein the gateway computer further comprises a gateway proxy and execution server for establishing a secure connection to the at least one host computer based on the permission data.

31. (Original) The system of claim 29 wherein the host computer further comprises a host proxy and execution server for establishing a secure connection between the at least one host computer and the gateway computer.

32. (Original) The system of claim 31 wherein the host proxy and execution server executes a command interpreter for executing commands.

33. (Original) The system of claim 29 wherein the client computer further comprises a downloadable executable interactive client (DEIC) for establishing a secure connection with the gateway computer.

34. (Original) The system of claim 33 wherein the downloadable executable interactive client (DEIC) comprises a Java applet.

35. (Original) The system of claim 29 wherein the gateway computer temporarily stores the principal-authenticating information.

36. (Previously Presented) A computer program product for use with a computer system,

the computer program product comprising a computer readable storage medium and a computer program stored therein for carrying out a process comprising:

(a)   obtaining by the client computer credentials for authorizing the principal from a validation enter;

(b)   establishing a first secure connection for exchanging data between a client and a network server;

(c)   transmitting from the client computer to the network server over the first secure connection the principal-authenticating credentials and the message;

(d)   transmitting the principal-authenticating credentials from the network server to the validation center;

(e)   transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials;

(f)   verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server;

(g)   establishing a second secure connection for exchanging data between the network server and a destination server based on the digital certificate; and

(h)   transmitting the message from the network server to the destination server over the second secure connection.

Evidence Appendix to Appeal Brief Under Rule 41.37(c)(1)(ix)

There is no evidence being relied upon by Appellant in this appeal.